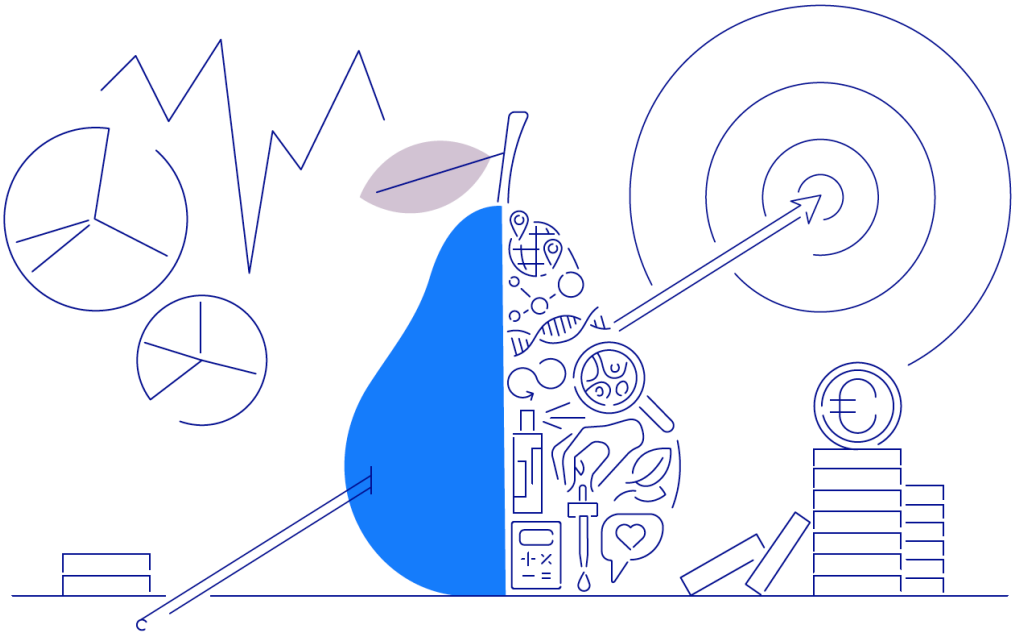
Innovatsiooni analüüsid 2022–2023

Plokiahel

November 2022



CIVITTA

TAL TECH

Euroopa Liit
Euroopa Regionaalarengu Fond

tuleviku heaks

Käesoleva analüüsi eesmärk on selgitada *plokiahela* tehnoloogiaid, nende rakendusvõimalusi ning tuua välja praktilisi kasutusvaldkondi ja kasutuslugusid. Ülevaade on suunatud Eesti ettevõtetele, tutvustamaks plokiahela põhimõtteid ja selle kasutamise praktikat. Kuigi plokiahel on eeskätt tuntud kui krüptoraha tehnoloogiate üks oluline osa, ei keskendu analüüs krüptorahale, vaid plokiahela teistele rakendusvõimalustele.

Analüüs koostati Ettevõtluse ja Innovatsiooni Sihtasutuse tellimusel CIVITTA Eesti AS ja Tallinna Tehnikaülikooli poolt perioodil september kuni november 2022.

Analüüsi autorid on Tallinna Tehnikaülikooli eksperdid Tanel Tammet ja Ahto Buldas. Analüüsi valmimist toetas Civitta Eesti AS projektijuht Piia Viks-Binsol.

Sisukord

1. Mis on plokiahelad?

Plokiahel[1] (inglise keeles *blockchain*) on levinud meetod jooksvalt täienevate andmekogude võltsimatuse tagamiseks ja eri osapoolte kasutuses olevate andmekogude koopiate jooksvalt sünkroonis hoidmiseks.

Kuigi plokiahelate kõige tuntum rakendusvaldkond on krüptoraha, siis tegelikult kasutatakse plokiahelaid väga paljudes tarkvarasüsteemides, mil ei ole krüptorahaga seost.

Võtame tavalise andmebaasisüsteemi, mille tabelitesse järjest lisatakse uusi kirjeid: olgu need näiteks rahaülekanded, ostud, ladustamine, laost kauba väljastamine vms. Alati on olemas potentsiaalne oht, et keegi, kel andmebaasile juurdepääs (näiteks andmebaasi administraator, pahatahtlik häkker või lihtsalt vigane tarkvara), muudab või kustutab tagantjärgi varasemalt salvestatud andmeid või lisab vale-andmeid, mis justkui oleks varem tegelikult lisatud. Ka siis, kui tegelikult on andmebaasis kõik korrektne, on olemas võimalus, et teised äriliselt huvitatud osapooled – näiteks kinnisvara ostjad/müüjad või panga klient – võivad andmed kahtluse alla seada ja nõuda nende õigsuse tõestamist. Samuti võivad kontrolliorganid nõuda tõendeid, et raamatupidamisdokumente ja muid andmeid ei ole tagantjärgi muudetud, kõrvaldatud või lisatud.

Kuidas plokiahel võltsimatust tagab? Peamine idee on lihtne ja kergesti realiseeritav. Plokiahela tarkvara koostab iga uue andmekirje (näiteks uus rida andmebaasis või uus Wordi või Exceli fail) jaoks lühikese võltsimatu kontroll-tekstijupi (*cryptographic hash*), millest võib mõelda kui unikaalsest sõrmejäljest. Seda väikest tekstijuppi nimetatakse *räsiks* ja tema võltsimatus tähendab, et praktiliselt võimatu on koostada etteantud räsi jaoks tagantjärgi tema jaoks sobivat alg-andmekirjet. Taoline räsi lisatakse siis igale uuele andmekirjele. Järgmise andmekirje räsi aga võetakse uuest andmekirjest, millele on lisatud ka eelmise andmekirje räsi. Nii koostatud andmekirjete ahela jaoks on alati võimalik teha kiire ja kindel kontroll, et ahelas olevaid andmeid ei

[1] https://en.wikipedia.org/wiki/Blockchain

Enamike andmekogude jaoks ei ole võltsimise oht väga suur, kuid suuremahulisi äriprotsesse toetavate rakenduste jaoks on ohud piisavad selleks, et võltsimatust tegelikult tagada.

Tüüpiliselt lisatakse plokiahelates igale uuele andmekirjele või dokumendile automaatselt nn **ajatempel**[2], mis markeerib selle kirje/dokumendi lisamise aega. Ajatempel võib omakorda olla kontrollitud ja allkirjastatud usaldatava kolmanda osapoole poolt, kes oma digitaalse allkirjaga kinnitab lisamise aja: selliseid ajatempleid kasutab näiteks Eesti digiallkirja süsteem. Kui andmeid lisavad mitmed erinevad osapooled, siis tüüpiliselt lisatakse plokiahelasse ka nende andmete lisaja identifikaator ja andmete **digiallkiri**[3]: selle koostab andmete lisaja tarkvara automaatselt ning saadab plokiahela süsteemi.

Plokiahelad on osutunud pea hädavajalikuks tehnoloogiaks **hajutatud andmebaasides**, ehk olukordades, kus andmeid lisavad, kasutavad ja kontrollivad sõltumatult korraga paljud osapooled ning igaühel on koopia tervest järjest täienevast andmekogust (inglise keeles *distributed ledger*, eesti keeles ***hajusraamat***[4]). Sel juhul tekivad kergesti erisused eri „koopiate“ vahel ning tekib küsimus, millised „koopiad“ on õiged ja millised valed. Plokiahel võimaldab iga „koopia“ korrektsust kontrollida, kuid ta ei ole üksi siiski piisav selleks, et osapooled suudaks alati kokku leppida, millised koopiad on õiged. Viimase probleemi lahendamiseks kasutatakse mitmesuguseid kokkuleppimis- ehk **konsensusprotokolle**[5].

Krüptoraha süsteemides nagu Bitcoin või Ethereum ongi kõigil osapooltel koopia kõigi seniste ülekannete andmebaasist, ning nad võivad sinna ise uusi ülekandeid lisada. Sellised lisandused saadetakse kõigile teistele osapooltele laiali. Seejuures tekivad nii eelmainitud võltsimatuse tagamise küsimused, mida lahendataksegi plokiahela tehnoloogiaga, kui ka ühiskokkuleppe leidmise küsimused, mille jaoks erinevad krüptoraha süsteemid kasutavad väga erinevaid algoritme. Üldiselt on ühiskokkuleppe saavutamine palju raskem ülesanne, kui võltsimatuse tagamine. Just ühiskokkuleppe leidmisele kulutavad krüptorahaga tegelevad arvutid väga palju aega, arvutusvõimsust ja elektrit: nn. **krüptoraha kaevandamine**[6] ongi krüptoraha ühiskokkuleppe algoritmide peamine osa.

Lisaks ühiskokkuleppe võimaldamisele sisaldavad keerukamad plokiahela süsteemid (mh pea kõik olulisemad krüptorahad) nn **nutilepinguid** (inglise keeles *smart contracts*[7]), mida kõik osapooled automaatselt kontrollimiseks käivitavad: nutileping on väike tükk tarkvara, mis kontrollib, kas hajusraamatusse lisatud andmerida on tegelikult lubatud ja korrektne. Kontroll saab arusaadavalt sõltuda ainult plokiahela senisest sisust (näiteks võib nutileping lihtsalt kontrollida, kas plokiahelas olevatest ülekannetest järeldub, et maksjal on piisavalt raha - plokiahela mõttes raha – või kas kirjes olev hind on plokiahelasse varem sisestatud tingimusega sätestatud koridoris vms).

[2] https://en.wikipedia.org/wiki/Trusted_timestamping
[3] https://en.wikipedia.org/wiki/Digital_signature
[4] https://en.wikipedia.org/wiki/Distributed_ledger
[5] https://en.wikipedia.org/wiki/Consensus_(computer_science)
[6] https://en.wikipedia.org/wiki/Cryptocurrency#Mining
[7] https://en.wikipedia.org/wiki/Smart_contract

Plokiahelate praktilise kasutamise planeerimisel on kõigepealt vaja aru saada, konkreetselt milliseid probleeme soovitakse plokiahelaga lahendada, ja valida seejärel sobiv plokiahela tehnoloogia variant. Kui mõnda probleemi õnnestub lahendada ilma plokiahelata, on selle jaoks mõistlik valida ilma plokiahelata lahendus. Keerukamat tüüpi plokiahelad on suhteliselt aeglased ning piiratud läbilaskevõimega. Kui vajadused ja sobivad plokiahela tüübid leitud, on järgmine samm sobiva olemasoleva realisatsiooni valik või – kõige lihtsamatel juhtudel – selle realiseerimine ise.

2. Plokiahelate tehnoloogiad

Jätkame eelmises peatükis antud plokiahela sissejuhatust täpsemate tehnoloogiliste detailidega. Baaspõhimõtetest paremaks arusaamiseks tasub siintoodule täiendavalt vaadata kahte videot ja katsetada ise ülamenüü lihtsa veebirakendusega lehelt https://andersbrownworth.com/blockchain/. Hea inglisekeelse detailülevaate plokiahelate tüüpidest, tehnoloogiatest ja rakendustest leiab näiteks artiklist Hitchhiker's Guide to the Blockchain[8].

2.1 Räsi

Iga plokiahela-süsteemi üks osa on võltsimatu ***räsi*** (*cryptograhic hash* ehk *krüptoräsi*) arvutamine igast uuest andmekirjest või uuest dokumendist. Krüptoräsist võib mõelda kui andmekirje või dokumendi unikaalsest *sõrmejäljest.* Kui anda ette mingi selline räsi, siis on praktikas võimatu mõelda välja või arvutiga genereerida selline andmekirje/dokument, mis annaks sellesama räsi. Ehk siis krüptoräsi on niiöelda ühesuunaline funktsioon: tekstist saab kergesti konstrueerida tema räsi, aga etteantud räsi jaoks ei saa leida talle sobivat teksti. Samuti ei saa praktiliselt koostada kahte erinevat teksti, millel oleks samad räsid.

Öeldes *ei saa*, mõtleme me tegelikult *ei ole realistlik.* Nimelt on lihtsa kõigi võimalike tekstide läbiproovimisega teoreetiliselt võimalik iga etteantud räsi jaoks erinevaid sobivaid tekste leida, seejuures tuleks aga läbi proovida astronoomiliselt palju tekste, mis ei ole ühelegi arvutisüsteemile jõukohane.

Kaasajal on levinuimad krüptoräsi algoritmid Riikliku Julgeolekuagentuuri NSA loodud **SHA-256** [9](mida kasutab ka Bitcoin ja Eesti ID-kaardi süsteem) ja selle pikem variant SHA-512: kummagi jaoks on tuhandeid eri realisatsioone ning kummagi algoritmi peetakse nii lühema kui keskpika tuleviku jaoks kindlaks. Kõigil suurematel programmeerimiskeeltel on teegifunktsioonid nende räside arvutamiseks. SHA-256 räsi pikkus on 32 baiti ehk tähemärki ning tema arvutamine on kiire: ühe tekstirea (ca 80 baiti) räsi leiab tava-arvuti umbkaudu

[8] https://netfuture.ch/2022/04/hitchhikers-guide-to-the-blockchain/
[9] https://en.wikipedia.org/wiki/SHA-2

ühe miljondiku sekundi jooksul ning ca 200 MB andmefaili räsi umbkaudu sekundi jooksul.

2.2 Ajatempel

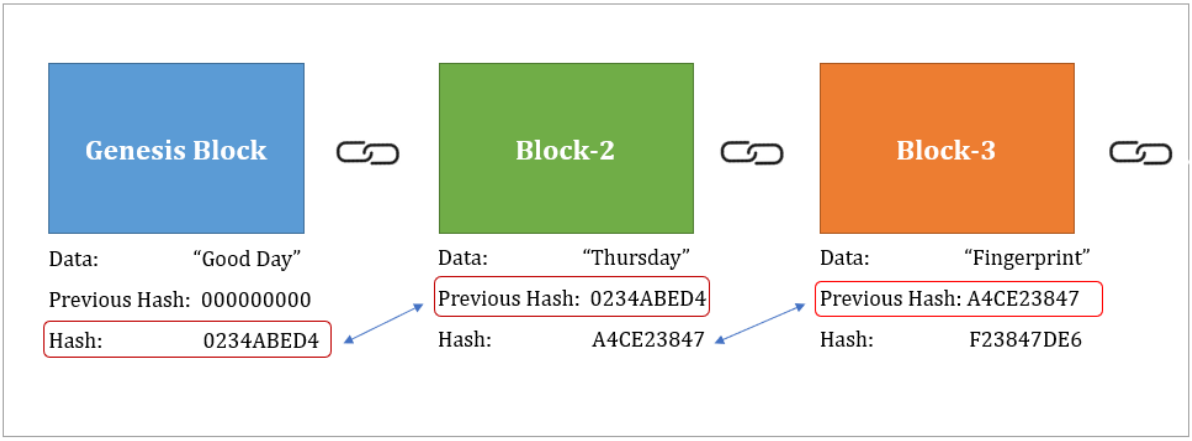
Enamik plokiahela süsteeme lisab igale uuele kirjele automaatselt **ajatempli**: see võib olla lihtsalt kokkulepitud formaadis kuupäev ja kellaaeg. Nagu ka muid plokiahela osi, ei saa ajatemplit tagantjärgi võltsida. Ajatempli võib anda ka kolmas, sõltumatu osapool, ning kinnitada ajatemplit automaatselt oma digiallkirjaga. Eestis on kaks sõltumatut taolise ajatempli teenuse pakkujat: ID Solutions AS ja Guardtime. ID Solutionsi ajatempel [10] lisatakse automaatselt kõigile Eesti eID süsteemi kaudu antud digitaalsetele allkirjadele. Guardtime ajatempli teenus oli selle ettevõtte esimeseks põhitooteks: nende ajatempli teenus (KSI Blockchain Timestamp[11]) salvestab etteantud räsi jaoks ajatempli Guardtime hallatavasse, kolmandate osapoolte poolt sõltumatult kontrollitavasse plokiahelasse.

2.3 Kirjed, plokid ja nende struktuur

Lihtsamat sorti plokiahelas on iga uus kirje (näiteks ülekanne, tehing, kauba liikumine laos, uus dokument) üks plokk. Plokid, nagu eelnevas kirjeldatud, on võltsimatuse tagamiseks kirje räside abil seotud ahelasse. Selle skeemi puuduseks on ahela tohutu pikkus, kui kirjeid on palju, ning ahela korrektsuse kontrollimise aeglus.

Räsi kasutamist kõige lihtsamat sorti plokiahela ehitamisel illustreerib joonis artiklist „*Blockchain key characteristics and the conditions to use it as a solution*[12]“: iga ploki räsi leitakse selle ploki „*Data*“ ja „*Previous Hash*“ väljade kokkuliitmisel saadud teksti jaoks:

[10] https://www.id.ee/artikkel/usaldusteenused-ajatempliteenus/
[11] https://guardtime.com/timestamping
[12] https://medium.com/swlh/blockchain-characteristics-and-its-suitability-as-a-technical-solution-bd65fc2c1ad1



Paljude väikeste kirjete puhul, eriti kui kiire kontrollimise võimalus on oluline, osutub mõistlikuks mitte siduda iga üksikut kirjet ahelasse, vaid pakendada mingi hulk kirjeid üheks plokiks kokku, ning siduda ahelasse sellised mitmekirjelised plokid. Räsi arvutatakse siis tervest plokist korraga.

Kontrolli-efektiivsuse tõstmiseks seotakse plokisisesed kirjed vahel omakorda ahelasse, kasutades seejuures mitte lineaarset ahelat, vaid räside hierarhilist puud nimega **Merkle puu**[13]. Bitcoini ülekande kirjed pakitakse reeglina ühte plokki, keskmiselt kaks tuhat kirjet plokis. Kirjed on omavahel seotud Merkle puu abil.

2.4 Arvestusraamat ja hajusraamat

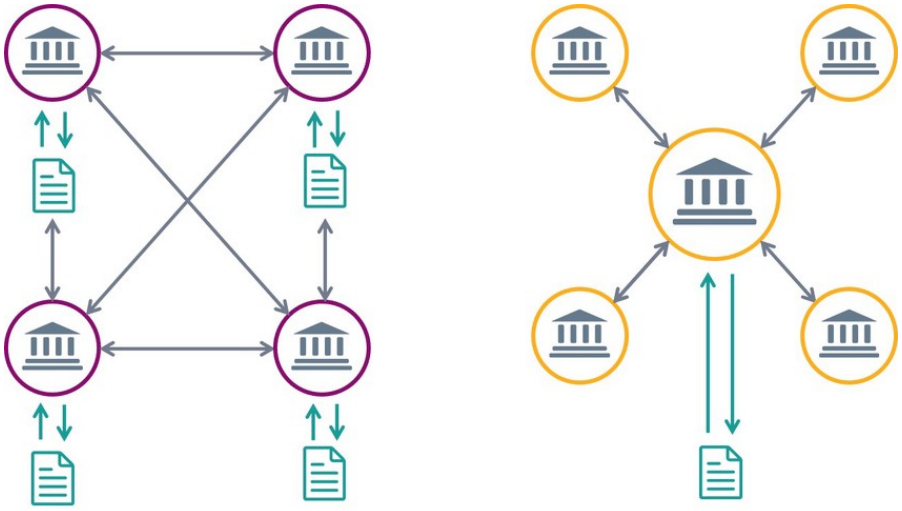
Jooksvalt täienevat andmekogu, mille võltsimatust plokiahelatega kaitstakse, nimetatakse **arvestusraamatuks** (inglise keeles *ledger*). Selle sisuks on tüüpiliselt kas andmebaasikirjed (mis ei pea olema konkreetses andmebaasisüsteemis, vaid võivad olla ka näiteks komadega eraldatud tekstiväljad) või dokumendifailid. Kui kirjeid lisavad sõltumatult mitmed osapooled, kellel kõigil on sellesama arvestusraamatu koopia, siis nimetatakse süsteemi **hajusraamatuks** (inglise keeles *distributed ledger*). Nagu varem märgitud, on hajusraamatu puhul kõige keerulisem küsimus koopiate sünkroniseerimine osapoolte vahel ehk **konsensuse** tagamine: osapoolte koopiad peavad olema identsed kuni ehk kõige uuemate kirjeteni, mis ei ole veel kõikidesse koopiatesse jõudnud.

Oluline on tähele panna, et tavalist andmebaasi või Exceli tabelit või dokumentide kataloogi on kõige lihtsam hallata keskselt üheainsa administraatori või organisatsiooni poolt, kes annab teistele juurdepääsu andmete lisamiseks ja küsimiseks, ning võib ka jagada selle andmekogu hetkeseisu koopiat. Sel juhul kaob ära konsensuse tagamise keerukas probleem: keskne haldur ongi see, kes otsustab, mis on arvestusraamatu õige sisu. Plokiahela lisamine arvestusraamatule tagab siis lihtsalt tema võltsimatuse.

[13] https://en.wikipedia.org/wiki/Merkle_tree

Enamik plokiahelat kasutavaid süsteeme nagu näiteks pangasüsteemid ja riiklikud registrid, ongi keskse halduriga.

Järgmine skeem artiklist „*Proof-of-PUF Enabled Blockchain: Concurrent Data and Device Security for Internet-of-Energy*[14]“ illustreerib hajusraamatu (a) ja tsentraliseeritud raamatu/andmebaasi (b) haldamise erinevust. Kui tsentraliseeritud süsteemi (b) puhul on üks keskne andmekogu, kuhu andmeid lisatakse, ja mis saadab eri koopiatele uuendusi, siis hajusraamatu puhul (a) võib iga andmekogu (hajusraamatu sõlm) ise oma andmekogusse andmeid lisada, ning saata need teistele samuti lisamiseks edasi. Sel juhul tekibki probleem, et kuidas tagada kõigi hajusraamatu sõlmede andmete sünkroonis hoidmine: kõigil sõlmedel peaks olema (kuni vähemalt viimaste lisandusteni) andmekogu teiste andmekogudega identne.



Vajadus hajusraamatu järele tekib tüüpiliselt olukordades, kus kas:

- ei **soovita põhimõtteliselt usaldada ühte keskset haldurit (näiteks panka)**: selliste süsteemide tüüpnäiteks on tavaline krüptoraha, nagu Bitcoin või Ethereum;
- või **tehnoloogilistel põhjustel**, kus üks server ei ole piisava võimsusega terve andmekogu haldamiseks: äärmusnäitena võib tuua ülisuured andmekogused, mida koguvad ning haldavad Google ja Facebook.

Hajusraamatuid jaotatakse üldiselt kahte liiki:

- **Mitteavalikud ehk loalised hajusraamatud** (*permissioned ledger*): arvestusraamatu koopiaid haldavad üksteist tundvad ja usaldavad osapooled, keda on tüüpiliselt vähe. Viimasel juhul on konsensuse saavutamine mõõdukalt keeruline ja ei nõua väga suuri arvutusressursse. Näiteks, kui hajusraamat seatakse sisse eeskätt tehnoloogilistel põhjustel

[14] https://www.researchgate.net/publication/347920052_Proof-of-PUF_Enabled_Blockchain_Concurrent_Data_and_Device_Security_for_Internet-of-Energy

(andmebaasi koormuse hajutamiseks), siis teeb seda enamasti üksainus organisatsioon, kes ise haldabki kõiki selle osi (inglise keeles *shards*).

- **Avalikud ehk loatud hajusraamatud** *(permissionless ledger*): igaüks võib soovi ja võimekuse korral asuda ühe koopia haldajaks, ning ise saata teistele osapooltele uusi andmekirjeid, eesmärgiga, et need jõuaks kõikidesse koopiatesse. Sel juhul on konsensuse saavutamine väga keeruline ja nõuab tihtipeale suuri arvutusressursse. Tüüpilised krüptoraha-süsteemid ongi loatud hajusraamatud: osapooled ei ole identifitseeritud, igaüks võib liituda. Loatu hajusraamatu kasutuselevõtt eeldab sisuliselt ka hajusraamatuga seotud krüptoraha kasutamist, millega motiveerida sõltumatute haldajate poolt tehtavat kontrollimis/konsensuse-leidmise tööd.

  - Kui ei ole tungivat vajadust loobuda ühest kesksest haldurist, on äärmiselt mõistlik mitte asuda kasutama hajusraamatut.
  - Kui hajusraamatut kasutada, siis tuleks võimaluse korral eelistada mitteavalikku hajusraamatut, mis võimaldab konsensust oluliselt lihtsamalt tagada.

2.5 Konsensus

Küsimus konsensusest tekib ainult hajusraamatu puhul, kus osapooltel on oma koopiad kogu arvestusraamatust ning nad saavad ise kõigile osapooltele lisamiseks uusi kirjeid saata. Konsensus tähendab tagamist, et need koopiad on kuni kõige viimaste uute kirjeteni osapooltel identsed. Üldistatult võib neid jagada kahte liiki:

- Klassikalised **leppeprotokollid** (inglise keeles *agreement protocols* ja *consensus algorithms*), mida tüüpiliselt kasutatakse tehnoloogilistel põhjustel hajutatud andmebaasides, ehk siis loalistes hajusraamatutes. Üldpõhimõttena hääletavad osapooled regulaarselt ühe ajutise usaldatava halduri / autentse koopia, keda kõik peavad mõnda aega järgima, kuni valitakse uus. Taolisi protokolle ja nende teostusi on väga palju, tuntumad nendest on Paxos[15] ja Raft[16]. Need protokollid töötavad kiiresti ja hästi, kuid ainult olukordades, kus osapooli ei ole väga palju. Osades loatutes hajusraamatutes, kus osapooli on palju, kasutatakse sarnase ideena nö ajutisi koalitsioone pooljuhuslikult valitud osapooltest.
- Niinimetatud **Nakamoto konsensus** (inglise keeles *Nakamoto consensus*): nimi tuleneb Bitcoini looja pseudonüümist „Nakamoto“.

[15] https://en.wikipedia.org/wiki/Paxos_(computer_science)
[16] https://en.wikipedia.org/wiki/Raft_(algorithm)

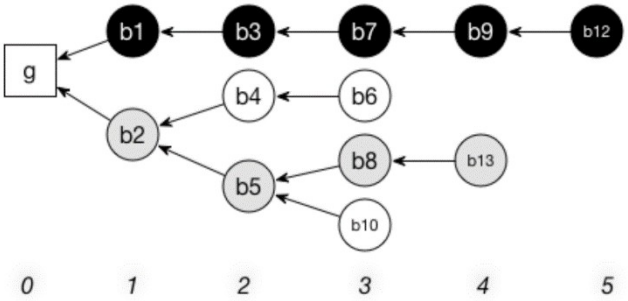
Enamik krüptorahasid kasutab selle konsensusalgoritmi erinevaid variante. Algoritmi põhi-idee on järgmine:

- Osapooltel võivadki olla veidi erinevad „koopiad“.
- Uue kirje lisamisel plokiahelasse tuleb mitme erineva „koopia“ olemasolul valida see, mis on antud plokiahela kriteeriumite järgi kõige „raskem“. Konkreetselt Bitcoini puhul on see tüüpiliselt kõige pikem plokiahel: täpsemalt selline, mille loomiseks kulutatud eeldatav arvutusmaht (mis on võrdeline kasutatud energiahulgaga) on suurim.

Nakamoto konsensusalgoritm on krüptorahade puhul tõepoolest pidevalt hoidnud üleval töötavat konsensust viisil, et vähemate plokkidega „koopiad“ muutuvad ebapopulaarseks, sinna kirjeid varsti ei lisata. Olulise miinusena on (a) igal ajahetkel viimaste kirjete/plokkide staatus ebaselge, st usaldada võib ainult kirjeid/plokke, mis on „piisavalt“ vanad, (b) algoritm nõuab reaalses töös tohutuid arvutusvõimsusi (oluline seotud termin: *proof of work*[17]), peamise eesmärgiga pidurdada uute plokkide lisamist: sisuliselt raisatud töö. Bitcoinis näiteks liidetakse uus plokk ahelasse keskmiselt kord kümnes minutis (plokk ise võib aga sisaldada palju kirjeid) ning vähem, kui pool tundi vanu plokke peetakse üldiselt ebausaldusväärseks. Teise näitena kasutab Ethereum erivarianti Nakamoto protokollist ja uus plokk luuakse ca iga kümne-paarikümne sekundi järel.

Mitmed krüptoraha süsteemid kasutavad kombinatsiooni spetsiifilistest leppeprotokollidest ja Nakamoto tüüpi konsensusest: nende realisatsioonid on keerulised ja praktilise töökindluse osas suurte mahtude korral on kahtlusi.

Võimaluse korral tuleks nö tavaliste plokiahelate (mitte krüptoraha kontekstis) korral kasutada loalist hajusraamatut väheste osapooltega ning võimalikult lihtsaid ja tuntuid klassikalisi leppeprotokolle. Mitmed laiemalt kasutatavad andmebaasi-tarkvarasüsteemid nagu Oracle, Postgresql ja SQL Server omavad sisse-ehitatud võimet andmebaasi loalises kontekstis hajutada, koos sisse-ehitatud algoritmidega nendevahelise konsensuse tagamiseks.



Ülalolev pilt jaluses viidatud artiklist[18] illustreerib Nakamoto-tüüpi konsensust olukorras, kus eri osapooltel on erinevad „koopiad“ plokiahelast ning uue ploki

[17] https://en.wikipedia.org/wiki/Proof_of_work
[18] „The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium“, C. Natoli, V. Gramoli, 2016.

lisaja **g** peab valima plokiahela eri hetkeseisu variantide **b1** ja **b2** vahel. Bitcoini kasutatav Nakamoto konsensus nõuab pikema ahelavariandi b1 valimist, keerulisem Ethereumi konsensus *Ghost* aga säilitab info äravisatud plokkide kohta ja nõuab nn „raskema“ ahelavariandi b2 valimist.

Kokkuvõttes tuleb märkida, et konsensuse küsimused on väga keerulised, eriti krüptorahades kasutatavate hajusraamatute ja loatute algoritmide korral, ning suurte andmemahtude ja paljude osapoolte korral toovad nad kaasa tõsiseid probleeme kasutamisel. Uurimistööd konsesus-algoritmide osas on väga aktiivsed nii ülikoolides kui plokiahelaid väljatöötavates ettevõtetes.

2.6 Nutilepingud

Suuremad plokiahela-süsteemid (mh enamik krüptoraha-süsteeme) sisaldavad *nutilepingute* (inglise keeles *smart contracts*) funktsionaalsust. Nutileping on väike tarkvaratükk, mille käivitamine kontrollib, kas kirje sisuks olev tegevus (näiteks rahaülekanne, ost vms) on lubatav. Mitte-lubatud toiminguid plokiahelas lihtsalt ei arvestata. Rahaülekannete puhul on reeglina üks kriteerium, et ülekandjal on kõigi temaga seotud plokiahela tehingute lõikes bilansis piisavalt raha. Keerulisemad programmid võimaldavad kontrollida näiteks plokiahelasse varem sisestatud hinnakoridorile vastavust või nõuet, et ülekannet võib teha ainult mingi konkreetse ajavahemiku jooksul. Kontrolliprogrammid saavad sisendiks plokiahela enda hetkeseisu, st nad ei saa arvestada infot, mida plokiahelas veel ei ole.

Plokiahela osapooled kontrollivad nutilepinguid, reaalselt käivitades plokiahelasse sisestatud programmid, ning loevad mittelubatud toiminguid mittetäidetuteks. Arusaadavalt nõuab selline kontrollimine küllalt palju arvutusvõimsust.

Enamasti kasutatakse nutilepingute jaoks Ethereumi krüptoraha plokiahelat, mis ongi kohandatud keerukamate lepingu-tarkvarade jaoks. Paraku on Ethereumisse nutilepingute sisestamine küllaltki kallis, alates paaristsajast dollarist kuni paarikümne tuhande dollarini. Seepärast kasutavad mitmed organisatsioonid nutilepingute plokiahelateks omaenda loodud ja hallatavaid piiratud juurdepääsuga plokiahelaid.

2.7 Krüptoraha ja NFT-d

Krüptorahad on reeglina avalikud hajusraamatud, kus igal osapoolel on oma „koopia“ kogu arvestusraamatust (kõigi osaliste tehtud kõik ülekanded aegade algusest) ja ta võib lisada sinna kirjeid. Kirjed on krüptoraha ülekanded stiilis „olen isik X ja kannan N raha isikule Y ja M raha isikule Z.“ Isikud on

identifitseeritud digitaalse avaliku võtmega [19], mis on anonüümne, ning nad kasutavad sama võtmepaari salajast võtit ülekannete allkirjastamiseks. Ülekannet loetakse korrektseks, kui kõigi seniste ülekannete läbivaatamisel on näha, et isiku X senine bilanss on piisav, ehk, tal on tegelikult üleantava summa järgi raha (peetakse silmas selle plokiahela arvestuslikku raha). Osapoolte tarkvara tegeleb neile saadetud ülekannete kontrollimise, registreerimise ja edasisaatmisega.

Nn *kaevandamine* tähedab (a) ülekannete korrektsuse kontrolli, (b) hulgast ülekannetest ploki moodustamist, ajatempli ja räsiga varustamist ning teistele osapooltele ploki laialisaatmist. Ploki moodustamine on kunstlikult keeruliseks tehtud: osapool peab leidma andmetele lisatava mõttetu sisuga tekstijupi (nn *nonce*), misjärel leitud räsi vastaks spetsiifilistele nõuetele (tüüpiliselt, peab algama etteantud arvu nullidega). Selle kunstlikult keeruliseks tegemise põhieesmärk on plokkide loomise tempo aeglustamine: Bitcoinis ca üks plokk kümnes minutis, Ethereumis ca kümnes sekundis. Osapool, kel õnnestub kontrollid teha, sobiv *nonce* leida ja lubatav räsi genereerida (seda otsingut nimetataksegi *kaevandamiseks:* inglise keeles *mining*), saab endale tasuks ise üle kanda auhinnaraha, mis on suhteliselt suur: selle auhinnaraha saamine ongi kaevandajate majanduslik eesmärk.

Krüptorahadel ei ole ühegi riigi või finantssüsteemi poolt garanteeritud väärtust: see on lihtsalt turul kujunevast nõudlusest tingitud, ning suhteliselt ebastabiilne[20].

NFT[21] (lühend fraasist *non-fungible token*) tehnoloogia sisuks on mitte ülekannete, vaid lihtsalt allkirjastatud ja spetsiifilises formaadis [22] omandusteadete paigutamine plokiahelasse, a la „Mina, John Smith, oman pilti veebiaadressil https://en.wikipedia.org/wiki/File:Mona_Lisa.jpg ja annan selle Jaan Sepa omandusse“. Sellistel teadetel ei ole juriidilist jõudu ei rohkem ega vähem, kui näiteks e-mailiga samasuguse teate saatmisel, kuid sellegipoolest leidub neile turg. Kindlasti tuleb arvestada, et NFT süsteemid ei kontrolli nendes teadetes olevate väidete vastavust tegelikkusele: internetist leitud meem ütleb *„the blockchain can't lie, but you can lie to the blockchain“.* Taoliste teadete plokiahelasse panekuks kasutatakse enamasti krüptoraha Ethereumi plokiahelat, mis sisaldabki nii ülekandeid, nutilepinguid, teateid jms erinevaid digiallkirjastatud tekstijuppe.

2.8 Olemasolev tehnoloogia ja tarkvara

Väljapool krüptoraha ja NFT-sid võiks praktikas kasutatavaid hajusraamatu-plokiahelasüsteeme jagada tehnoloogia mõttes kahte suurde klassi:

[19] https://en.wikipedia.org/wiki/Public-key_cryptography
[20] https://coinmarketcap.com/
[21] https://en.wikipedia.org/wiki/Non-fungible_token
[22] http://erc721.org/

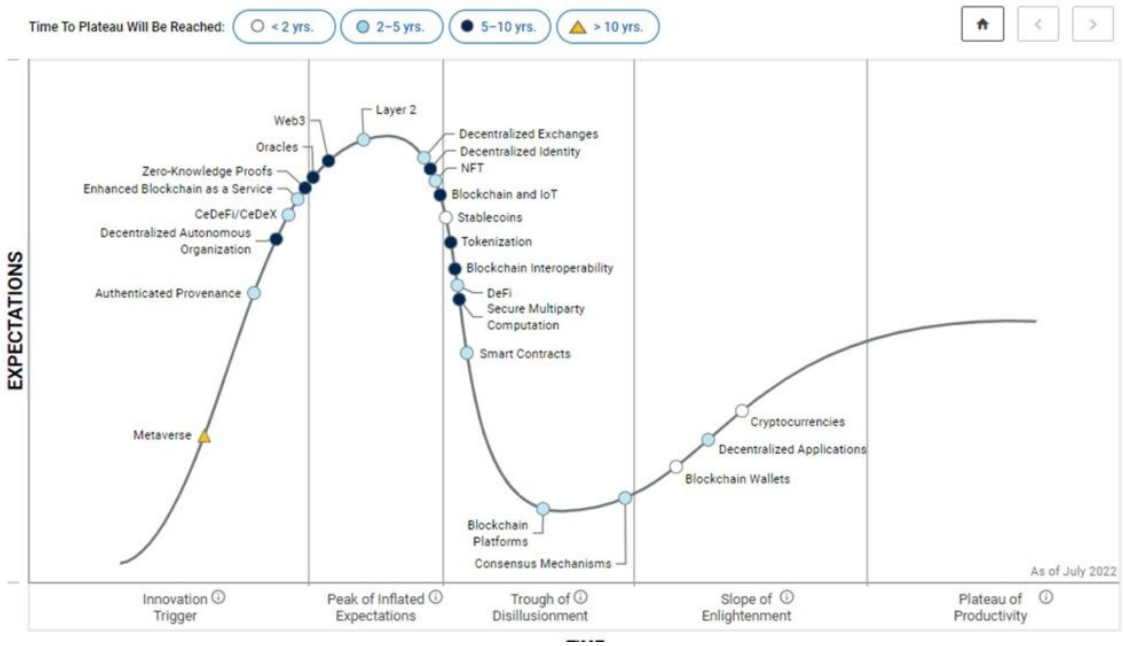
- Süsteemid, mis kasutavad mõnda suuremat tuntud avalikku krüptoraha-plokiahelat omaenda mitte-krüptoraha info salvestamiseks. Selleks kasutatakse enamasti mõnda sorti nutilepinguid, mida saab neisse plokiahelatesse salvestada. Peamine kasutatav plokiahel on mõnda aega olnud Ethereum, mis on aga muutunud vähegi suuremate andmemahtude jaoks liiga kalliks. Alternatiivina tasub vaadata Cardano süsteemi (lisaks allpool).
- Süsteemid, mis loovad enda plokiahela: enamasti piiratud juurdepääsuga. Tüüpiliselt kasutavad need süsteemid mõnda olemasolevat tarkvarasüsteemi taoliste plokiahelate loomiseks. Taolisi valmisehitatud tarkvarasüsteeme on saadaval palju, ning nende kõikide loetlemine ei oleks siin otstarbekas; toome välja ainult mõned tähtsamad punktid.
    - Üheks olulisemaks valmisehitatud taoliseks tarkvarasüsteemiks peetakse hetkel vabavaralist *Hyperledger Fabric* [23]süsteemi (vaata ka ülevaadet wikipediast[24]) mida arendatakse aktiivselt ja paljude osapoolte ühisprojektina, koordinaatoriks *Linux Foundation*. Projekti toetavad väga suured ettevõtted, mh IBM, Intel, J. P. Morgan, Wells Fargo jne.
    - Populaarsest tarkvarahoidlast *github.com* leiab suure hulga erinevaid, sh ka lihtsamaid vabavaralisi plokiahela-tarkvarasüsteeme.
    - Lisaks tasub märkimist, et suurimate krüptorahade – näiteks Bitcoin ja Ethereum – jaoks kasutatavad levinumad tarkvarasüsteemid on samuti vabavaralised.
    - Enda rakenduse tegemise kontekstis tasub vaatamist ka Cardano[25] krüptoraha tarkvara: Cardano projektis on pööratud palju tähelepanu süsteemi protokollide, tarkvara-osade ja terviksüsteemi enda laiema kasutamise lihtsustamisele.

[23] https://www.hyperledger.org/use/fabric
[24] https://en.wikipedia.org/wiki/Hyperledger
[25] https://cardano.org/

3. Probleemid

Plokiahela kasutuselevõtu kavandamise üks kõige suuremaid raskusi on objektiivse ja adekvaatse informatsiooni saamine plokiahelate põhimõtete ja praktiliste rakendusvõimaluste kohta. Plokiahelatega seotud krüptorahade kiirete tõusude, kõrge volatiilsuse ja spekulatiivse iseloomu tõttu on plokiahelate teema olnud aastaid äärmiselt populaarne. Plokiahelate kohta produtseeritakse pidevalt artikleid ja uudiseid, millest enamus on kas sensatsioonilist laadi, ülioptimistlikud, nö ajakirjanduslik vaht või siis kantud mõne isiku või organisatsiooni huvidest. Sellest infohulgast on konkreetsete vajaduste jaoks kasulikku ja usaldusväärset informatsiooni väga raske leida.

Siinkohas on sobilik vaadata Gartneri publitseeritavat erinevate plokiahelatehnoloogiate avaliku populaarsuse nn *hype-cycle*'[26]t 2022 aasta suvest: horisontaaltelg näitab tehnoloogia populaarsus- ja küpsusastet ajas.



Järgnevas vaatame juba konkreetseid probleeme, millega tuleb arvestada, jättes seejuures välja spetsiifiliselt krüptoraha kasutamisega seotud riskid: viimaste

[26] https://blogs.gartner.com/avivah-litan/2022/07/22/gartner-hype-cycle-for-blockchain-and-web3-2022/

kohta annab hea detailse ülevaate näiteks viidatud S&P artikkel[27]. Hea üldise ülevaate plokiahelatega seotud riskidest annab artikkel *A survey on blockchain technology and its security*[28].

Plokiahela-tehnoloogia kasutamise planeerimisel on mõistlik selgelt eristada kahte erinevat taset:

- Plokiahela kasutamine võltsimatuse saavutamiseks: kas enda ehitatud rakendus, mis seob andmebaasi-kirjeid või faile *räsi* abil tagantjärgi-kontrollitavasse ahelasse, või siis mõne olemasoleva plokiahela-süsteemi kasutamine samaks otstarbeks.
- Plokiahela kasutamine – lisaks eelmisele – hajusraamatu pidamiseks, ehk siis erinevate osapoolte sõltumatult lisatavate andmebaasi-kirjete sünkroniseerimine kõigi osapoolte jaoks identseks ja ühiselt aktsepteeritavaks plokiahelaks.

2.1 Võltsimatuse tagamise probleemid

Esimene, lihtsam tase ei ole seotud eriliste probleemidega, tingimusel, et selleks ei püüta kasutada olemasolevaid krüptoraha-põhiseid plokiahelaid, näiteks Ethereumi. Viimasel juhul ilmnevad kohe keerukamat tüüpi, hajusraamatu põhise plokiahela probleemid.

Esimese taseme plokiahela potentsiaalne probleem on suurte mahtude korral tekkida võivad jõudlusraskused. Kui andmeid lisatakse väga kiires tempos, siis vajadus kirjed ahelasse siduda raskendab lisamise paralleliseerimist. Mõõduka lisamistempo juures, näiteks paar kirjet sekundis, olulisi tehnoloogilisi probleeme ja keerukusi ei teki.

Mittetriviaalne, kuid mitte ka väga keerukas, on vajadus luua lisaks lahendus, mis võimaldaks potentsiaalset võltsimist ka tegelikult tuvastada, ehk siis suudaks plokiahelat ja selle kirjeid sõltumatult kontrollida. Jällegi, suurte andmemahtude korral on selline lahendus mittetriviaalne, samuti vajab läbimõtlemist küsimus, kuidas tagada plokiahela kui terviku säilimine ja võltsimatus, näiteks välistades terve plokiahela võimaliku asendamise võlts-plokiahelaga. Viimase küsimuse lahendamise üks levinud viise on plokiahelas olevate räside ja ajatemplite regulaarne (näiteks kord päevas/nädalas/kuus) publitseerimine sõltumatutele andmekandjatele, kasvõi paber-ajalehes publitseeritava väikese kuulutusena.

Samuti tuleb arvestada, et senised plokiahelatehnoloogiad ei käsitle piisavalt pika perspektiivi turvaohtu, mis tuleneb kasutatavate krüptoalgoritmide (tüüpiliselt SHA-256) nõrgenemisest, ehk nn. *pikaajalist turvalisust* (*long-term security*). Teisisõnu, eksisteerib väike risk, et mingil hetkel suudetakse realistliku aja jooksul konstrueerida alternatiivseid (võlts) tekste, mis vastavad ahelas olevale räsile, kaotades sellega täielikult plokiahela tõendusväärtuse. Selle

[27] https://www.spglobal.com/_assets/documents/ratings/research/101563051.pdf
[28] https://www.sciencedirect.com/science/article/pii/S2096720922000070

riskiga on seotud küsimus, et kuidas vahetada tulevikus nõrgaks muutuv räsifunktsioon uue ja turvalisema vastu. Lisadetaile leiab näiteks artiklist „*Long-Term Secure Time-Stamping Using Preimage-Aware Hash Functions*[29]“.

[29] https://link.springer.com/chapter/10.1007/978-3-319-68637-0_15

2.2 Hajusraamatu probleemid

Teise taseme plokiahela – hajusraamatu – kasutuselevõtt on aga oluliselt keerukam ülesanne ja tekitab suure hulga probleeme, mistõttu soovitame seda kasutada ainult juhul, kui selleks on objektiivne vajadus, mida ei saa mõnel lihtsamal viisil lahendada.

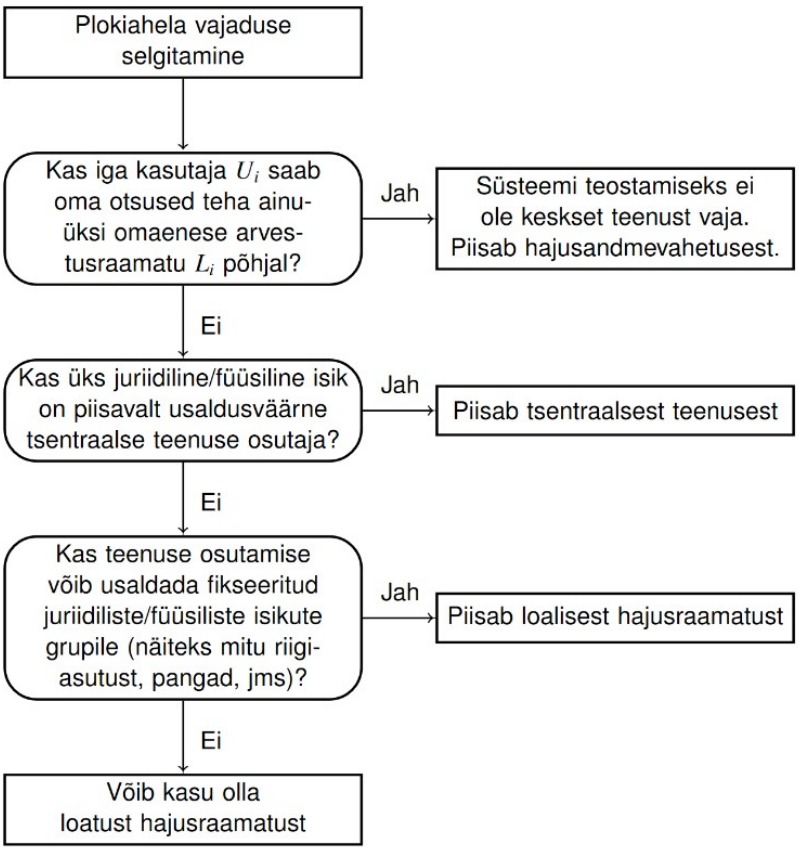
Esitame siin mittetäieliku loetelu tekkivatest probleemidest, millest kõik peale esimese puudutavad eeskätt loatuid ehk avalikke plokiahelaid. Loaliste ehk piiratud hulga usaldatavate osapoolte jaoks sobivad tehnoloogiad võimaldavad töödelda palju suuremaid andmemahte ja palju kiiremini, seega on nad üldjuhul mõistlikum valik. Ei ole juhus, et järgmistes peatükkides toodud reaalsetes kasutuslugudes kasutatakse enamasti just loalisi ehk piiratud hulgale osapooltele kättesaadavaid plokiahelaid.

- Küsimus, kas kasutada mõnda olemasolevat hajusraamatut (näiteks Ethereum) või luua oma hajusraamat, ja viimasel juhul, milline täpselt. Nii olemasolevaid hajusraamatu-süsteeme kui nende ise ehitamiseks sobivaid tehnoloogiaid ja tarkvaralahendusi on saadaval väga palju ja väga erinevaid, seejuures on neil kõigil nii miinused kui plussid.
- Olemasolevad loatud ehk avaliku hajusraamatu tehnoloogiad ei ole võimelised efektiivselt töötlema väga suuri andmemahte: nad ei sobi juhul, kui andmeid on juba väga palju, ega juhul, kui andmeid väga kiires tempos lisatakse. Uued, efektiivsemad tehnoloogiad on alles uurimis- ja katsetamisjärgus.
- Spetsiifiliselt krüptorahade – mis kasutavad nn loatut ehk avalikku hajusraamatut - üks suurimaid tehnoloogilisi probleeme on ühiselt usaldatavas andmehulgas kokkuleppimise raskus. Näiteks Bitcoinis ei ole mõistlik usaldada ühtegi andmeplokki, mis on vähem kui ca tund aega tagasi moodustatud. See tähendab, et reaalses kaubanduses, kus ülekande kontrolliks on vähe aega, ei saa Bitcoini tüüpi krüptoraha kasutada.
- Variant eelmisest probleemist on kõigi loatute hajusraamatute puhul usaldusväärse kokkuleppimise töö- ja ajamahukus, mis toob kaasa plokiahelasse lisamise kulud, mis seda töö- ja ajamahukust kontrollivatele osapooltele kataks. Varem oleme maininud, et näiteks Ethereumi plokiahelasse – kuhu saab sisestada nn tarku lepinguid ja mis töötab ka kiiremini, kui Bitcoini tüüpi plokiahel – on ühe kirje lisamise hind (sõltuvalt „lepingutarkvara“ keerukusest) paaristsajast dollarist kuni paarikümne tuhande dollarini. Selle põhjus on vajadus, et väga paljud osapooled sõltumatult teostaks kõik vajalikud kontrollid ja seejuures käivitaks plokki lisatava „targa lepingu“ tarkvara.
- Loatute hajusraamatute kasutamise potentsiaalne oht on plokkide kontrollijate ehk kaevandajate võimalik majandusliku huvi langus ja soov mitte oma tööd jätkata. Sel puhul võib plokiahel liikuda sisuliselt ühe või

paari allesjäänu monopoolse kontrolli alla (kaotades sellega usaldusväärsust) või muutub ahelasse uute kirjete lisamine üldse võimatuks. Sarnaselt on olemas potentsiaalne oht, et mingi plokiahel hargneb erinevateks variantideks, ning täielikku konsensust (ehk milline on ühiselt aktsepteeritud variant) enam ei saavutatagi. Taoliste sotsiaalmajanduslike riskide suurusi ja võimalikke konsekventse ei ole piisavalt uuritud.

Ka loalised plokiahelad, mille sotsiaalmajanduslikud riskid on väikesed ja tehnoloogiline võimekus suurem, on siiski keerulised süsteemid, mille planeerimine, tehnoloogia valik, ehitamine ja rakendamine ei ole lihtsad ülesanded.

Järgnev hajusraamatu sobivuse ja valikute plokkskeem on toodud Riigi Infosüsteemi Ameti (RIA) tellitud ja AS Cybernetica koostatud uuringus *Krüptograafiliste algoritmide elutsükkel*[30] aastast 2017, ning ta on endiselt adekvaatne.



[30] https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf

4. Valdkonna arengu ülevaade

4.1 Plokiahelate ja hajusraamatute algus

Võltsimatuse eesmärgil ehitatud lihtsamat tüüpi plokiahelad on küllalt vana tehnoloogia, mis pärineb eelmise sajandi seitsmekümnendatest ja kaheksakümnendatest aastatest. Suurte mahtude kiireks töötlemiseks sobivad lahendused on hilisemad: üks varasemaid selliste lahenduste pakkujaid, Eesti ettevõte Guardtime, alustas nendega ca 2007. aastal.

Suur osa loaga ehk piiratud kasutusega hajusraamatute tehnoloogiast pärineb hajutatud andmebaaside valdkonnast: esimesed siiani kasutuses lahendused töötati välja eelmise sajandi üheksakümnendatel aastatel.

Plokiahela mõiste – ja loatute ehk avalike plokiahelate tehnoloogia laiemalt – algas esimeste lihtsamate süsteemidega eelmise sajandi kaheksakümnendatel ja jõudis laiema avalikkuse teadvusse seoses kaasaegse krüptoraha leiutamisega aastal 2009: anonüümne grupp autoreid pseudonüümiga „Nakamoto“ pakkus välja Bitcoini lahenduse põhimõtted, vabalt kasutatava tarkvara ja käivitas reaalselt Bitcoini plokiahela. Bitcoini väärtuse esimene kiire tõus aastatel 2011-2013 tekitas selle vastu suurema avaliku huvi, ning motiveeris hulga uute, Bitcoinist veidi erinevate põhimõtte-nüanssidega krüptoraha-projektide käivitamise, nagu näiteks Litecoin, Dogecoin ja Ethereum.

2014. aastal initsieeriti esimesed NFT-de projektid, mille eellaseks oli Bitcoini võimaldatav nn „*colored coin*“ ehk niiöelda privaatraha suurema plokiahela koosseisus (muuseas kasutas seda ka Eesti ettevõte Funderbeam). NFT projektid ja NFT-dega spekuleerimine muutusid väga populaarseks ca 2018. Viimastel aastatel on paljud ettevõtted katsetanud NFT-de väljalaskega nö privaatraha loomiseks (mh Eesti single.earth ja koos.io): rakendusviis, mis ei ole NFT-de algne eesmärk, kuid milleks ta võib siiski sobida.

4.2 Arengud alates aastatest 2017-2018

Bitcoini väärtuse järgmisel kiire kasvu perioodil 2017-2018 tekkis avalikkuses suur huvi nii krüptorahade kui plokiahelate vastu laiemalt. Käivitati suurtes kogustes erinevate põhimõtetega krüptorahasid (leht coinmarketcap.com jälgib pea kümmet tuhandet erinevat krüptoraha) ja püüti aktiivselt leida loaga ja loatute hajusraamatute rakendusi muudes valdkondades.

Samas hakkasid selguma ka loatute plokiahela-tehnoloogiate praktilised piirangud: eeskätt raskused suurte andmekoguste ja kiires tempos andmete lisamise olukorras, samuti loatute plokiahelate hajusraamatu sünkroonis hoidmiseks tehtavad suured kulutused, mis muudavad Bitcoini ja Ethereumi tüüpi loatute hajusraamatute kasutamise kalliks ja ebaefektiivseks. Suurem konkreetsem areng selle probleemi leevendamiseks on 2022. aasta sügisel rakendunud Ethereumi krüptoraha ja plokiahela uus versioon[31], mis kasutab loatu hajusraamatu sünkroniseerimiseks senise, väga energiamahuka ja kuluka nn *proof-of-work* [32] asemel palju efektiivsemat *proof-of-stake* [33] põhimõtet. Juba varem on paljud väiksemad krüptorahad asunud kasutama erinevaid kombinatsioone *proof-of-work* ja *proof-of-stake* põhimõtetest.

Valdkonna areng viimasel viiel aastal ongi suundunud eeskätt hajusraamatu-tehnoloogia arendamisele: uute, senistest oluliselt efektiivsemate konsensus-protokollide otsimisele ja nendega katsetamisele tegelikes plokiahelates, enamasti uute krüptorahade kontekstis. Selliste uuringute üks spetsiifiline haru on näiteks stabiilse väärtusega ja suuri ülekannete mahte võimaldavate krüptorahade arendamine: head näited on Euroopa keskpanga digieuro uurimisprojekt[34] ja Facebooki juhtimisel arendatav krüptoraha Libra, praeguse nimega Diem[35]: mõlemid on uurimis- ja katseprojektid, mitte reaalselt kasutatav krüptoraha.

Eesti ettevõtte Guardtime arendatav projekt Alphabill, mida kirjeldab artikkel „*An Ultra-Scalable Blockchain Platform for Universal Asset Tokenization: Design and Implementation*“[36] on hea näide sellelaadsest uurimis- ja katseprojektist, mille eesmärk on nimelt suurte andmemahtude kiire ning odava töötlemise võimaldamine (teisisõnu *skaleeruvuse* saavutamine) hajusraamatu jaoks, võimaldades sadu tuhandeid transaktsioone sekundis. Ehkki projekti fookuses on krüptorahaga võrreldes palju laiem rakendussfäär, sisaldab Alphabill ka krüptoraha, sest praktiliselt iga loatu hajusraamatu süsteem on sunnitud emiteerima/kasutama omaenda krüptoraha, motiveerimaks hajusraamatu sünkroonis hoidmise tööd.

Konkreetsemaks minnes võib välja tuua kahte olulisemat uurimissuunda:

- skaleeruvuse saavutamine dekompositsiooni abil (*sharding*)
- plokiahelate ühendamine (*kompositsioon*) liitsüsteemideks

[31] https://ethereum.org/en/upgrades/merge/
[32] https://en.wikipedia.org/wiki/Proof_of_work
[33] https://en.wikipedia.org/wiki/Proof_of_stake
[34] https://www.eestipank.ee/press/keskpanga-digieuro-uurimisprojekt-naitas-plokiahela-tehnoloogia-uusi-voimalusi-26072021
[35] https://en.wikipedia.org/wiki/Diem_(digital_currency)
[36] https://ieeexplore.ieee.org/abstract/document/9834329

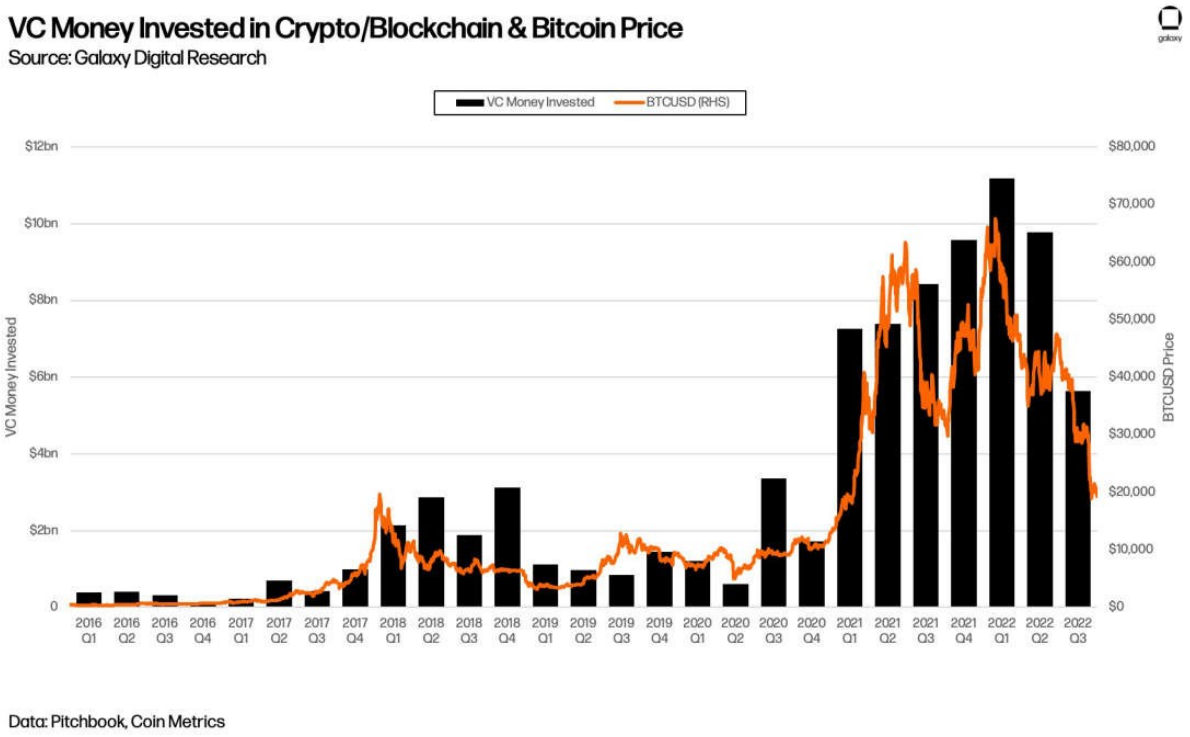
Efektiivse dekompositsiooni olemasolu sõltub plokiahela kui andmestruktuuri omadustest, ning ei ole alati võimalik. Dekompositsioonile esitatavad lisanõuded (näiteks komponentide ja/või plokiahelas osalevate üksuste piiratud arvutusvõimsus ja sidevõimekus) võivad tekitada keerulisi turvalisuse probleeme[37].

Artikli „Emerging Trends in Blockchain Technology and Applications: A Review and Outlook[38]“ andmetel on plokiahela uuringuid kajastavate publikatsioonide arv on Web or Science Core Collection andmebaasi põhjal (mis kajastab ainult osa maailmas avaldatud artiklitest) vahemikus 2013 kuni 2020 kiiresti kasvanud: aastatel 2013 – 2015 alla saja artikli, aastal 2019 juba 3250 artiklit, aastal 2020 veidi vähem, 2716 artiklit.

4.3 Investeeringud, rakendused ja web 3

Plokiahela tehnoloogiate arendamisse tehtavaid investeeringuid ei ole lihtne mõõta, kuna plokiahela-tehnoloogiad on seotud nii puhtalt krüptorahadesse investeerimisega, uute krüptorahade väljalaskega, baastehnoloogia arendamise ja plokiahelate rakendamisega: erinevad, kuid omavahel seotud valdkonnad. Analüüsifirma Galaxy toob välja hinnangulised investeeringumahud plokiahela-iduettevõtetesse[39], millest nähtub, et investeeringute maht on sünkroonis Bitcoini turuväärtusega: pärast Bitcoini tugevat tõusu aastatel 2017-2018 investeeriti krüpto/plokiahela iduettevõtetesse ca 8 miljardit dollarit aastas, seejärel langesid investeeringud ca 2 miljardi dollarini aastas, kuni uue tõusuni 2021 ja languseni 2022 teises pooles (ca 30 miljardit dollarit kogu 2022 kohta). Järgnev joonis viidatud Galaxy uuringust näitab kvartaalseid investeeringuid krüpto/plokiahela iduettevõtetesse (vasak telg) ja võrdleb neid Bitcoini hinnaga (parem telg):

[37] https://near.org/papers/nightshade/
[38] https://www.sciencedirect.com/science/article/pii/S1319157822000891
[39] https://www.galaxy.com/research/insights/crypto-and-blockchain-venture-capital-q3-2022/



Paralleelselt uute baastehnoloogiate loomisega on paljud suuremad ettevõtted maailmas asunud uurima võimalusi hajusraamatute kasutamiseks praktilises töös: peatükid 5 ja 6 toovad välja hulga valdkondlikke näiteid.

Vaatamata aktiivsele uurimis- ja katsetamistööle ei ole loatute, avalike hajusraamatute efektiivistamise valdkonnas praeguseks veel jõutud tulemusteni, mis oleksid piisavalt kiired, odavad ja stabiilsed, et neid reaalsetes suuri mahte ja kiirusi nõudvates IT süsteemides väljapool krüptoraha kasutada. Samal põhjusel ei ole ka krüptorahad veel jõudnud sellise tehnoloogilise tasemeni, kus neid saaks kasutada massilisteks igapäevasteks arveldusteks.

Suuremad hajusraamatute rakendusnäited tööstuses ja panganduses kasutavad praegu loalisi, piiratud ligipääsuga plokiahelaid.

Hea detailse ülevaate plokiahela-tehnoloogiate arengutest leiab 2022 aasta artiklist „*Emerging Trends in Blockchain Technology and Applications: A Review and Outlook*“[40].

2021. aasta jooksul muutus populaarseks mõiste **Web 3**[41], mis sisuliselt tähistab detsentraliseerimise ideoloogiat koos lootusega, et plokiahelate tehnoloogiad võiksid aidata seniste suurte tsentraliseeritud süsteemide (Google, Facebook, pangad jne) asemel luua detsentraliseeritud süsteeme, näiteks loatute, avalike hajusraamatute abil. Web 3 ei tähista seega ühtegi konkreetset tehnoloogiat, protokolli või rakendust, vaid ideoloogiat. Arusaadavalt on selline puht-ideoloogiline olemus koos Web 3 sagedase mainimisega viisil, mis tekitab mulje,

[40] https://www.sciencedirect.com/science/article/pii/S1319157822000891
[41] https://en.wikipedia.org/wiki/Web3

nagu oleks tegu reaalse süsteemi või tehnoloogiaga, tekitanud hulgaliselt möödarääkimisi ja vaidlusi.

5. Plokiahela rakendused maailmas

Kõige tuntum plokiahelate kasutusvaldkond on krüptoraha. Erinevaid krüptorahasid [42]on loodud kümneid tuhandeid; tegelik likviidne väärtus on ehk ca tuhandel. Seejuures on reaalselt olulised ehk ainult paarkümmend suuremat.

Plokiahela tehnoloogiate kasutusvaldkond on tunduvalt laiem, kui krüptorahadel. Järgnevas kirjeldame nende olulisemaid kasutusvaldkondi maailmas väljapool krüptoraha sfääri.

Selles peatükis ei kajasta me *lihtsate plokiahelate* kasutusjuhte arvestusraamatu või dokumendikogu võltsimatuse saavutamiseks: neid kasutusjuhte käsitleme järgnevas, Eesti praktikate peatükis. Järgnevas vaatame eeskätt hajusraamatu kasutusjuhte: neis on olulised nii võltsimatus kui erinevate osapoolte andmekoopiate sünkroonis hoidmine.

5.1 Kasutusjuhtude eesmärgid ja üldised tähelepanekud

Peamine probleem, mida keerukamate plokiahelate kasutusjuhud lahendavad, on **usaldusväärne andmevahetus** paljude osapoolte vahel. Tüüpiline näide on tarneahelad, mis algavad toormaterjalide tootmisega, nende transpordiga tööstusesse, seal komponentide valmistamisega ning transpordiga järgmise taseme tootmisüksustesse jne, kuni toodang jõuab lõpptarbijani. Osapoolte suur hulk, erinevad huvid ja tööpõhimõtted muudavad komponentide jälgimise kogu tarneahelas äärmiselt keeruliseks. Kuidas ehitada süsteem, kuhu kõik osapooled pidevalt infot sisestaks ning sealt vajalikku infot leiaks? Kuidas motiveerida osapooli taolise süsteemiga liituma? Mida teha, kui osapooled vahetuvad (mis on omakorda pidev protsess)?

Plokiahelate kasutamine logistikas ja tarneahelates on eeskätt motiveeritud nimelt sellestsamast ülesandest: luua ühine transporditavate toodete andmebaas, mida pidevalt täiendatakse toodete hetkeasukohtade, sihtkohtade jms olulise infoga. Hajusarvestusraamat on üks võimalik lähenemine, mis annab

[42] https://coinmarketcap.com/

eri osapooltele sarnased õigused ja võimalused infot lisada ja kasutada, ning võimaldab nutilepingute abil elementaarset kontrolli sisestatava info üle. Samuti tõstab plokiahelana organiseeritud hajusarvestusraamat osapoolte usaldust andmete vastu.

Kui lihtsate plokiahelate, mille eesmärgiks on võltsimatuse saavutamine, on praktikas laialt levinud, näiteks finantssüsteemides ja IT valdkonnas, siis hajusraamatute laiem kasutamine väljapool krüptoraha valdkonda on tihtipeale veel kuigivõrd eksperimentaalse iseloomuga. Järgnevates peatükkides toodud kasutusjuhtude näited kasutavad pea kõik loaga ehk piiratud ligipääsuga hajusraamatuid, mida on oluliselt lihtsam rakendada kui loatuid ehk avalikke. Samas ei ole selge, et nende näidete ärilisi eesmärke ei saaks realiseerida ka üldse ilma hajusraamatuta, nagu seda teevad pea kõik „harilikud“ lahendused analoogilistele probleemidele. Ärilised ja tehnoloogilised põhimõtted hajusraamatute valdkonnas on alles katse- ja selgumisfaasis.

Kasutatava tehnoloogia ja tarkvara osas vaata ülevaadet varasema „Plokiahelate tehnoloogiad“ alapeatükist „Olemasolev tehnoloogia ja tarkvara“.

5.2 Töötlev tööstus

Naftatootjad ja -töötlejad British Petroleum, Statoil ja Shell lõid 2018. aastal ühiselt kauplemisplatvormi VAKT[43], mis asendab konventsionaalseid paberlepinguid plokiahelas olevate nutilepingutega. Süsteemi eesmärk on efektiivistada naftaga kauplemise protsesse.

[43] https://www.vakt.com/

VAKT kasutab mitteavalikku plokiahelat, ning osapoolte kriitiline info plokiahelas

> "*Our founding partners recognised a problem that required collective action: the physical post trade process was reliant on manual, complex, repetitive and therefore error-prone processes.*
>
> *By coming together and conducting their post trade work on a blockchain-enabled platform, they saw that these problems could be solved, and that they could better protect the value of their trades*."
>
> > *"Meie asutajad leidsid, et järgmine problem vajab ühiselt lahendamist: müügijärgsed tegevused nõudsid keerulist ja üksluiset käsitööd, ning olid seetõttu vea-altid.*
> >
> > *Viies ühiselt oma müügijärgsed tegevused plokiahela tehnoloogiat kasutavale platvormile, suutsid nad nimetatud probleemid lahendada ja oma müükide väärtust paremini kaitsta."*
>
> Tsitaat VAKT veebilehelt.

on krüpteeritud. Konkreetselt kasutab VAKT JP Morganis loodud – ja hiljem ettevõttele ConsenSys edasi müüdud - Quorum-i tarkvara, mis kasutab omakorda Ethereumi tehnoloogiat omaenda plokiahela loomiseks.

Täiendava tööstusliku rakendusnäitena toome välja, et Eesti ettevõtte Guardtime tehnoloogiat kasutab võltsimatuse saavutamiseks ja tarneahelate haldamise optimeerimiseks muuhulgas ka USA militaarvaldkonna suurfirma Lockheed Martin[44].

5.3 Veondus ja laondus

Logistikavaldkonna võibolla suurim ja tuntuim plokiahela reaalses kasutuses projekt on Maerski ja IBMi juhtimisel loodud Tradelens[45] platvormi rakendamine.

Tradelens-i kasutamise üks osa on tollideklaratsioonide digiteerimine. Digitaalsed tollideklaratsioonid allkirjastatakse digitaalselt koostaja poolt ning salvestatakse plokiahelasse, mis mh muudab nad võltsimis- ja vaidlustamiskindlaks.

[44] https://www.newsbtc.com/news/lockheed-martin-blockchain-guardtime-federal/
[45] https://www.tradelens.com/

Tradelens kasutab omakorda varasemas mainitud Hyperledger Fabric vabatarkvara. Maerski platvormi kasutuslugu[46] kirjeldab näitena Highland Foods-i probleeme ja nende lahendusi Tradelens abil järgmiselt:

> *„Through the TradeLens API integration, we are able to perform auto data synchronisation into our EDI system 3 times a day, which enables more effective inventory management. We are also able to plan our warehouse schedule at the bonded area better, via real-time ETA updates and notifications to the task owners*."
>
> *„Integreerides Tradelens API oma süsteemi, suudame andmeid sünkroniseerida oma EDI süsteemi kolm korda päevas, mis võimaldab laosüsteeme efektiivsemalt majandada. Reaalajas ETA uuenduste ja tähelepanujuhtimiste abil suudame oma ajakavasid samuti paremini planeerida,"*
>
> Sunghub Song,
>
> Team Leader, Information Planning Team Highland Foods Co. Ltd

Tradelensi kasutab praegu [47] üle 90 erineva osapoole (20 neist tollid ja sadamad) ning süsteemi kaudu on praeguseks töödeldud üle 360 miljoni saadetise.

Vaatamata senisele positiivsele meediakajastusele teatas Maersk 2022 aasta novembris[48], et sulgeb Tradelens'i projekti 2023 esimese kvartali lõpuks. Põhjusena toodi välja projekti vähene kommertsedu.

5.4 Info- ja kommunikatsioonitehnoloogia

Infotehnoloogia ettevõtted on plokiahela tehnoloogiaga kõige tihedamalt seotud, kuid reeglina kas (a) teenuste ja tarkvara pakkujana, või (b) krüptoraha kaevandajana/vahendajana, mitte niivõrd mõne plokiahela-süsteemi omaette lõpptarbijana. Näiteks oleme juba mitmel korral maininud, et Eesti IT ettevõtetest on plokiahela teenusepakkumisele ja tarkvara arendamisele rajatud Guardtime ärimudel.

[46] https://www.maersk.com/news/articles/2021/07/27/how-blockchain-technology-is-beefing-up
[47] https://dataconomy.com/2022/06/best-enterprise-blockchain-examples-2022/#Maersk_Cargo_shipping
[48] https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens

Sarnaselt IT ettevõtetele pakuvad mitmed telekomi-ettevõtted spetsiifilisi plokiahela-põhiseid teenuseid.

Näiteks hispaania ettevõte Telefónica pakub dokumentide/failide võltsimatuse-tagamise ajatempliga plokiahela-põhist teenust[49] sarnaselt Eesti Guardtime teenusele. Nimetatud teenus kasutab lihtsat tüüpi plokiahelat, milles ei ole hajusraamatut.

Deutsche Telekom (DT) ja selle tütarettevõte T-Systems pakuvad plokiahela-tehnoloogiate konsultatsiooniteenuseid ning on mitme oma katsetamisprojekti kaudu tegevad ka krüptoraha valdkonnas: DT toetab ja on ostnud märgatava hulga Celo[50] krüptoraha, mis mh seob mobiilikasutajate telefoninumbrid nende identiteediga Celo krüptoraha plokiahelas. DT plaanib luua SMS-teenuseid, mille abil Celo plokiahelas olevat infot kontrollida saaks. Samuti on DT osaline [51]Ethereumi uues plokiahela-versioonis ühe kontrollimis-sõlmena.

5.5 Pangandus

Pangandus ja finantsteenused üldisemalt on olnud üks peamisi plokiahelate kasutamise valdkondi, mis on loomulik, kuna suurimad ja tuntumad plokiahela-süsteemid ongi krüptorahad. Teisest küljest on enamiku krüptorahade eesmärk nimelt vältida vajadust usaldusväärsete kesk-organisatsioonide järele, milleks rahanduses ongi pangad. Viimast – pankadega konkureerivat - lähenemist tähistatakse teminiga *Decentralized finance* ehk *DeFI.*

Plokiahelate rakendusi pankades tasub jagada kahte liiki:

- Lihtsamad rakendused tagavad kriitiliste andmebaaside võltsimatuse ja auditeeritavuse, ilma hajusarvestusraamatuta.
- Keerukamad rakendused sisaldavad hajusarvestusraamatut.

Üks suuremaid panganduses kasutatavaid hajusarvestusraamatu-süsteeme on JP Morgani juhtimisel loodud *Liink*[52], varasema nimega *Interbank Information Network (IIN)*, mille eesmärk on pakkuda alternatiivne variant makse-info vahetamiseks finantsinstitutsioonide vahel. Liinki süsteemiga on ühinenud üle

> „*Liink enables institutions to exchange payment-related information quickly and securely and addresses challenges that result in increased costs and delays.*
>
> *We established Liink to find more efficient ways to transfer data through custom applications*.“
>
> *"Liink võimaldab institutsioonidel oma makseinfot kiiresti ning turvaliselt vahetada, vähedades seeläbi hinda tõstvaid ja viivitusi tekitavaid tegureid.*
>
> *Lõime Liinki selleks, et pakkuda erirakenduste jaoks kiiremaid andmevahetus-võimalusi. „*
>
> Tsitaat J.P. Morgani veebilehelt
> https://www.jpmorgan.com/onyx/liink

49
b
50
51
st
52

400 panga üle maailma, mh enamik suurimatest 50st pangast maailmas. Liinkiga on ühinenud ka Eestis tegutsevad Nordea ja SEB. Liink kasutab alustehnoloogiana JP Morganis arendatud loalist varianti Ethereumi plokiahela tarkvarast.

Mitmed keskpangad maailmas on asunud uurima võimalusi krüptoraha väljalaskeks, kuid siiani on need projektid uurimistöö ja eksperimentide tasemel. Kindlasti tasub märkimist Euroopa keskpanga digitaalse euro[53] uurimisprojekt, millega on seotud ka Eesti panga oma eksperimentaalprojekt[54] ning projektis kasutatava KSI Cash [55] tehnoloogia kaudu Eesti ettevõte Guardtime.

Detsentraliseeritud panganduse DeFI – ehk siis pankadele alternatiivi pakkumise – osas on olemas mitmeid väiksemaid edulugusid. Põhinäitena tuuakse enamasti Ethereumi plokiahelat kasutav DAI stabiilne krüptoraha ja sellega tegelev MakerDAO[56] organisatsioon, mis võimaldab DAI krüptovääringut kasutada intressiga laenamiseks.

[53] https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html
[54] https://www.eestipank.ee/press/eesti-panga-eksperiment-uuris-keskpanga-digiraha-tehnilisi-voimalusi-plokiahelal-13122021
[55] https://guardtime.com/ksi-cash
[56] https://makerdao.com/en/

6. Plokiahelate praktika Eestis

Sarnaselt eelnevale valdkondlike kasutusjuhtude ülevaatele, jätame siin peatükis välja puhta krüptoraha-majanduse: kaevandamine, krüptorahasse investeerimine, müük jne. Samuti ei püüa peatükk katta kõiki plokiahela kasutusjuhte või ettevõtteid Eestis.

Spetsiifilise ülevaate krüptorahade tunnustamise teemadest Eesti riiklikus kontekstis leiab rahandusministeeriumis aastal 2016 koostatud dokumendist „Analüüs virtuaalvääringute võimaliku tunnustamise ja kasutamise poliitika väljatöötamiseks“[57]. 2022. aasta riiklikud seisukohad ja nõuded krüptorahade kasutamise osas on kirjeldatud Euronewsi artiklis[58] *„Estonia used to be a crypto pioneer but is now clamping down on crypto licenses. This is why“*.

6.1 Riigiasutused

Eesti riigiametid kasutavad plokiahelat mitmete oluliste registrite võltsimatuse tagamiseks. Esimesi katseid alustati juba 2008, ning 2012 seoti plokiahelaga esimese riikliku registrina pärimisregister. Praeguseks on võltsimise vastu plokiahela abiga kaitstud hulk registreid majandus-, justiits-, sise-, rahandus- ja sotsiaalministeeriumi haldusalas, muuhulgas järgmised[59]:

- Digilugu ja digiretsept tervise infosüsteemis.
- Äriregister ja pärimisregister.
- Mitmed kohtusüsteemi registrid, mh digitoimik.
- Mitmed Politsei- ja Piirivalveameti andmebaasid.
- Kinnistusraamat.
- Riigi teataja.
- Avalikud teadaanded.

[57] https://www.fin.ee/media/2767/download või https://eelnoud.valitsus.ee/main/mount/docList/8e283f23-ef97-4dfa-8d3b-8edef96b50d9#mwVakkyQ
[58] https://www.euronews.com/next/2022/06/01/estonia-used-to-be-a-crypto-pioneer-but-is-now-clamping-down-on-crypto-licenses-this-is-wh
[59] https://toolbox.estonia.ee/assets/423218 ja https://e-estonia.com/wp-content/uploads/2020mar-nochanges-faq-a4-v03-blockchain-1-1.pdf

Erinevate allikate kinnitusel kasutavad need registrid (millest ükski ei ole hajusraamat) Guardtime KSI plokiahelat, mille jaoks riigi Registrite ja Infosüsteemide Keskus (RIK) on loonud ka spetsiaalse X-tee liidese[60]. Konkreetsed plokiahela kasutamise tehnoloogilised valikud neis registrites on erinevad: näiteks pärimisregistris lisatakse iga üksik kanne plokiahelasse eraldi, mitmetes teistes aga lisatakse kandeid plokkide kaupa. Kõigis on kasutusel ka ajatempel, mis tuleb KSI plokiahelast.

Riigisüsteemis on loodud seoseid ka suuremate rahvusvaheliste registritega, näiteks teatas[61] RIK 2022 alguses „Registrite ja Infosüsteemide Keskus (RIK) aitas Eesti Patendiameti intellektuaalomandi registrid liita Euroopa Liidu kaubamärkide ja tööstusdisainide plokiahela võrguga, et kaubamärkide teavet saaks partnerriikide registritega jagada kiirelt ning turvaliselt hajusandmebaasi kaudu.“

Samuti on riigiasutuste infosüsteemid kasutanud – ja tõenäoliselt kasutavad ka praegu – väiksemaid ja lihtsamaid enda ehitatud plokiahela-süsteeme enda vähemkriitiliste andmekogude võltsimatuse tagamiseks.

6.2 Ettevõtted

Sarnaselt eelkirjeldatule kasutavad mitmed Eesti ettevõtted plokiahelat oma sisemiste andmekogude võltsimatuse tagamiseks. Ühe konkreetse näitena võib tuua SEB panga süsteemilogid.

LHV pank asutas aastatel 2015/2016 tütarettevõtte Cuber Technology, mis emiteeris omaenda stabiilset/tagatud krüptoraha *Cuber token* ning pakkus sellele Tallinnas paaris kohas reaalset väikesemahulist kasutusvõimalust. Aastal 2022 tütarettevõte likvideeriti, sest reaalset tegevust ettevõttes enam ei toimunud.

Iduettevõtete osakutega kauplemise börsisüsteemi looja Funderbeam[62] kasutas oma tegevuse esimestel aastatel osakute/tehingute jaoks Bitcoini plokiahelat, kuid hiljem loobus sellest[63].

Hetkel on Eestis vähemalt kaks ettevõtet, kes kasutavad plokiahelas olevaid NFT tokeneid kui nö *sotsiaalset ehk privaatset raha*:

- Single.Earth[64] on väike startup-ettevõte, mis fokuseerib looduskeskkonna säilitamisele ja motiveerib selles suunas tegutsevaid maaomanikke enda emiteeritud krüptoraha-taolise MERIT NFT tokeniga, mis kasutab Solana plokiahelat. Tsitaat Single.Earth veebilehelt: „*Every token represents and protects 'the work nature does' to keep the planet habitable (called ecosystem services). The tokens are issued to landowners based on the*

[60] https://www.ria.ee/et/uudised/e-riik-2018-x-tee-vahendab-sellest-nadalast-alusteenusena-plokiaheldust.html
[61] https://www.rik.ee/et/news/rik-loi-uhenduse-euroopa-liidu-kaubamarkide-plokiahela-vorguga
[62] https://www.aripaev.ee/uudised/2016/12/07/eesti-ettevotted-naevad-blockchainis-voimalust
[63] https://www.funderbeam.com/help/how-does-funderbeam-use-blockchain/
[64] https://www.single.earth/

ecological value of their lands for as long as nature is preserved.“ Ehk *„Iga token esindab ja kaitseb ’looduse tööd’, hoidmaks meie planeeti eluks sobilikuna (ehk ökosüsteemi teenused). Token-eid antakse maaomanikele, kes säilitavad seal olevat loodust, vastavuses nende maa ökoloogilisele väärtusele“.* Tegevusi selle NFT tokeniga saab näha näiteks Solscan MERIT tokeni lehelt[65].

- koos.io[66] on väike startup-ettevõte, mis arendab teenust, mille abil ettevõtted ja muud organisatsioonid saavad emiteerida omaenda krüptoraha-sarnast privaatset NFT tokenit, sarnaselt eelmainitud MERIT tokenile. Eestis kasutab nende abiga loodud US TOKENit klientide ja taksojuhtide motiveerimiseks Forus takso[67]. Tokeneid lubatakse viie aasta pärast vahetada Forus takso osaluseks (kokku 30% ettevõtte osakutest).

Täiendavat infot plokiahela kasutusjuhtude ja edulugude kohta Eestis leiab järgmisest, võrgustike peatükist: sealkirjeldatut ei hakka me siin peatükis kordama.

[65] https://solscan.io/token/HjUMVG3yQK7uMTq1TerG6C8JzAjRvMdYCoX7ZUzKTgjH
[66] https://koos.io/
[67] https://forus.ee/en/uus-forus-taxi-teeb-kliendid-ja-teised-ettevottesse-panustajad-kaasomanikuks

7. Võrgustik

Euroopa Liidul on plokiahela-strateegia [68] veebileht, kus regulaarselt avaldatakse olulisemaid uudiseid ja infot relevantsete projektide kohta. Muuhulgas käivitas Euroopa Liit aastal 2018 üle-Euroopalise plokiahela (katse)projekti EBSI[69] . **EBSI** on mõeldud nii avalikule sektorile kui ettevõtetele, kuid on hetkel endiselt pilootfaasis, ning ettevõtteid seni otse liituma ei kutsuta. Eesti on küll EBSI liige, kuid mitte aktiivne osaleja EBSI plokiahela kasutamisel.

Nagu oleme eespool maininud, osalevad Euroopa Keskpanga digieuro uurimisprojektis [70] ka Eesti Pank ning ettevõte Guardtime.

Samuti on Euroopa Liit käivitanud usaldusväärsete plokiahela-rakenduste loomisele suunatud assotsiatsiooni INATBA[71]

Eestis tegeletakse plokiahelatega kahes väga erinevas kontekstis (a) krüptoraha kaevandamine, sellesse investeerimine, müük, NFT jms (b) plokiahela tehnoloogiate arendamine ja teenuste pakkumine laiemas kontekstis. Siin käsitleme nimelt viimast konteksti, jättes spetsiifiliselt krüptorahaga tegelemise ja nö tava-NFT-de väljalaske vaatluse alt välja.

Peamine plokiahela-tehnoloogia arendaja ja teenusepakkuja Eestis on **Guardtime**[72]. Guardtime on Eesti tarkvara-arendusettevõte, millel üle 100 töötaja ning kontorid Tallinnas, Tartus ja mitmetes välisriikides. Guardtime esialgne fookus ja põhiteenus on kolmandate osapoolte poolt kontrollitava, võltsimatu ajatempli-teenuse pakkumine, mis kasutab nende eesmärkide saavutamiseks enda ehitatud ja hallatavat KSI plokiahelat[73]. KSI plokiahel on Euroopa Liidu EIDAS-e direktiivi järgselt auditeeritud ja akrediteeritud, olles esimene seliselt akrediteeritud usaldusteenus üldse. Praegusel hetkel on Guardtime koostöös Tallinna Tehnikaülikooliga arendanud välja uudseid plokiahela süsteeme laiemaks kasutamiseks (näiteks Alphabill[74]) ning pakub rahvusvahelisel turul mitut liiki plokiahela teenuseid, mida muuhulgas kasutab hulk Eesti riiklikke registreid kirjete võltsimatuse saavutamiseks. Guardtime peamine arengufookus on hetkel suurte andmemahtude ja väga sagedasti lisatavate kirjete efektiivne haldamine plokiahelate abil. Nimelt see

[68] https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy
[69] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home
[70] https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html
[71] https://inatba.org/
[72] https://guardtime.com/
[73] https://guardtime.com/timestamping
[74] https://ieeexplore.ieee.org/abstract/document/9834329

skaleerimisprobleem on siiani osutunud põhiraskuseks plokiahelate kasutamisel tööstuses ja logistikas.

Akadeemilise poole pealt tegeleb Eestis plokiahelate uurimise, rakendamisvõimaluste analüüsi ja koolitustega nii **Tallinna Tehnikaülikool** (konkreetselt vaata **infosüsteemide gruppi**[75]) kui **Tartu Ülikool** (**Arvutiteaduse instituut**[76]).

Nii akadeemilisi uuringuid kui kommertsiaalset tarkvaratootmist edendav **AS Cybernetica** on varasemas samuti töötanud välja plokiahela-süsteeme ja nende tehnoloogiat, konkreetselt süsteemi Cuculus[77] , mis küll ei ole enam kasutuses, ning omab selles valdkonnas arvestatavat võimekust, sh ka analüüside koostamise vallas. AS Cybernetical on üle 150 töötaja, ning kontorid nii Tallinnas kui Tartus.

Eesti Krüptoraha Liit[78] seob mitmeid krüptoraha ja plokiahelatega tegelevaid organisatsioone Eestis ning toob mh välja ka teenuseid, mida tema liikmed pakuvad.

Ettevõtete osas on arvestatav kompetents eelmises peatükis mainitud NFT-de kasutuse arendajatel, väikestel startup-tarkvara-ettevõtetel **Single.Earth** ja **Koos.io**.

Eesti Pank on koostöös teiste riikide keskpankadega osalenud digieuro uurimisprojektis[79], tsitaat: „Eksperiment näitas, et plokiahela tehnoloogiale tuginev uudne digitaalse euro tehnoloogia on hästi skaleeritav ehk vajadusel saab kerge vaevaga suurendada digieuroga tehtavate maksete arvu.“

Riigiasutuste osas on tõenäoliselt suurim plokiahela-tehnoloogia **kogemus Registrite ja Infosüsteemide Keskusel (RIK)**, mille haldusalas on hulk KSI plokiahelaga tagatud riiklikke registreid.

Mitmed advokaadibürood pakuvad juriidilisi nõustamisteenuseid krüptoraha ja plokiahelat puudutavates küsimustes. Näited: **Njord Law** [80] ja **Hedman Legal** [81].

Lisaks on Eestis mitmeid väiksemaid uurimisgruppe ja eksperte, kes tegelevad plokiahela temaatikaga ning konsultatsiooniteenustega (näiteks Dymaxion[82]).

Kokkuvõtteks võib öelda, et Eestis leidub arvestatav kompetents nii plokiahela kasutusvõimaluste analüüsiks kui ka reaalsete plokiahelat kasutavate süsteemide ehitamiseks, seejuures on praktiline kogemus aga peamiselt lihtsamate, võltsimatust tagavate plokiahelate ehitamisel. Hajusraamatu-süsteemide kasutamise, eriti loatute ehk avalike hajusraamatu-süsteemide loomise näiteid väljapool krüptoraha ei ole palju. See vastab kogemustele teistes

[75] https://taltech.ee/en/is
[76] https://cs.ut.ee/en
[77] https://link.springer.com/content/pdf/10.1007/BFb0055749.pdf
[78] https://www.kryptoraha.ee/
[79] https://www.eestipank.ee/press/keskpanga-digieuro-uurimisprojekt-naitas-plokiahela-tehnoloogia-uusi-voimalusi-26072021
[80] https://www.njordlaw.com/et/kruptovaluutad-plokiahel-ja-fintech
[81] https://hedman.legal/et/teenused/plokiahel-ja-krupto/
[82] https://www.dymaxion-mfssia.com/

riikides: nii tehnoloogiliste kui sotsiaalmajanduslike piirangute ja keerukuste tõttu on hajusraamatu praktiline kasutamine praeguste plokiahela-tehnoloogiate juures küllalt raske ülesanne ning enamikke praktilise infovahetuse probleeme saab lahendada lihtsamalt. Plokiahela-tehnoloogia eduka edasise arengu korral võib nende kasutamine laieneda.